John J. Nelson (SBN 317598)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
280 S. Beverly Drive
Beverly Hills, CA 90212
Telephone: (858) 209-6941
Email: jnelson@milberg.com

Attorney for Plaintiffs and the Proposed Class

IN THE UNITED STATES DISTRICT COURT

FOR THE CENTRAL DISTRICT OF CALIFORNIA

SALVATORE SPINA, individually and on behalf of all others similarly situated, Plaintiff, v. KEENAN & ASSOCIATES, Defendant.	Case No.: **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Salvatore Spina ("Plaintiff"), individually and on behalf of all others similarly situated, brings this class action against Defendant KEENAN & ASSOCIATES ("Defendant" or "Keenan"), and alleges as follows:

I. JURISDICTION AND VENUE

1. This Court has subject-matter jurisdiction pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d) because (1) the matter in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, (2) the action is a class

action, (3) there are members of the proposed Class who are diverse from Defendant, and (4) there are more than 100 proposed Class members. This Court has supplemental jurisdiction over state law claims pursuant to 28 U.S.C. § 1367 because they form part of the same case or controversy as the claims within the Court's original jurisdiction.

2. This Court has general personal jurisdiction over Defendant because Defendant is a resident and citizen of this district, Defendant conducts substantial business in this district, and the events giving rise to Plaintiff's claims arise out of Defendant's contacts with this district.

3. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(1) & (2) because Defendant is a resident and citizen of this district and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this district.

II. PARTIES

4. Plaintiff Salvatore Spina is a resident and citizen of California.

5. Defendant KEENAN & ASSOCIATES is a California stock corporation with its principal place of business at 2355 Crenshaw Blvd., Suite 200, Torrance, CA 90501.

III. FACTUAL ALLEGATIONS

KEENAN & ASSOCIATES

6. Defendant Keenan represents that it "provides innovative insurance and budgetary solutions for schools, public agencies and health care organizations" and it

claims to be "the experts you can rely on when it comes to risk management, claims services, and technology."[1]

7. Keenan is an insurance brokerage company that provides insurance related risk management and claims services throughout California and to clients across the country.

8. Plaintiff and Class members are customers of Defendant's clients.

9. Plaintiff and Class members provided certain Personally Identifying Information ("PII") and Protected Health Information ("PHI") to clients of Defendant, which clients then provided the information to Defendant.

10. As a sophisticated insurance provider with an acute interest in maintaining the confidentiality of the PII and PHI entrusted to it, Defendant is well-aware of the numerous data breaches that have occurred throughout the United States and its responsibility for safeguarding PII and PHI in its possession. Defendant represents to consumers and the public that it "takes [its] privacy responsibility very seriously and is committed to protecting [private information] in a manner consistent with applicable law...."[2] Further, Defendant represents that it possesses robust security features to protect PII and PHI and that it takes its responsibility to protect PII and PHI seriously:

> We do not sell your personal information to third parties, other than in connection with a merger, sale, or other transfer of organizational assets where Personal Information held by us about our clients is among the assets transferred.

[1] https://www.keenan.com/About

[2] https://www.keenan.com/Privacy-Statement

> ***
> We have implemented measures reasonably designed to protect and secure your Personal Information from accidental loss, misuse, and from unauthorized access, use, alteration, and disclosure.[3]

11. Keenan maintains a separate Privacy Policy and Notice for California residents on its website, where it states, among other things, that "We will disclose Personal Information for a business purpose only to service providers, or, where required by law, or in response to valid legal process compelling disclosure."[4]

The Data Breach

12. According to Defendant, on August 27, 2023, Defendant "discovered certain disruptions occurring on some Keenan network servers."[5]

13. Defendant "learned that an unauthorized party gained access to certain Keenan internal systems at various times between approximately August 21 and August 27, 2023, and that the unauthorized party obtained some data from Keenan systems."[6]

14. The compromised data includes affected persons' "name, date of birth, Social Security number, driver's license number, passport number, general health information, and health insurance information." [7]

---

[3] *Id.*

[4] https://www.keenan.com/CCPA

[5] https://www.keenan.com/Notice-of-Security-Incident

[6] *See* Data Breach Notification Letter, attached hereto as Exhibit 1.

[7] *Id.*

15. According to a notice of data breach filed with the Attorney General of Maine, the Data Breach has affected 1,509,616 individuals ("Data Breach").[8]

16. Defendant began notifying affected persons on January 26, 2024.[9]

17. Defendant's letter also offered free credit monitoring services to those potentially impacted by the breach.

18. Defendant did not state why it was unable to prevent the Data Breach or which security feature failed.

19. Defendant did not state why it did not contact affected persons about the breach until five months after discovering the breach.

20. Defendant failed to prevent the data breach because it did not adhere to commonly accepted security standards and failed to detect that its databases were subject to a security breach.

Injuries to Plaintiff and the Class

21. On or around January 26, 2024, Plaintiff received a breach notification from Defendant indicating that his Personally Identifiable Information ("PII") and Personal Health Information ("PHI") was compromised during the Data Breach.[10] According to the notification letter, the Data Breach exposed Plaintiff's date of birth,

[8] https://apps.web.maine.gov/online/aeviewer/ME/40/21846091-dc71-4ecc-9db8-a3be3e84a7d0.shtml

[9] *Id.*

[10] *See* Exhibit 1.

Social Security number, passport number, driver's license number, health insurance information, and other general health information.

22. After the Data Breach, Plaintiff has received phishing emails and/or spam calls daily.

23. In response to the Data Breach, Plaintiff has placed a freeze on his credit and has contacted all three credit bureaus to place fraud alerts on his accounts.

24. Plaintiff is very concerned about the theft of his PII and PHI and has and will continue to spend substantial amounts of time and energy monitoring his credit status.

25. As a direct and proximate result of Defendant's actions and omissions in failing to protect Plaintiff's PII and PHI, Plaintiff and the Class have been damaged.

26. Plaintiff and the Class have been placed at a substantial risk of harm in the form of credit fraud or identity theft and have incurred and will likely incur additional damages, including spending substantial amounts of time monitoring accounts and records, in order to prevent and mitigate credit fraud, identity theft, and financial fraud.

27. In addition to the irreparable damage that may result from the theft of PII and PHI, identity theft victims must spend numerous hours and their own money repairing the impacts caused by this breach. After conducting a study, the Department of Justice's Bureau of Justice Statistics found that identity theft victims "reported

spending an average of about 7 hours clearing up the issues" and resolving the consequences of fraud in 2014.[11]

28. In addition to fraudulent charges and damage to their credit, Plaintiff and the Class will spend substantial time and expense (a) monitoring their accounts to identify fraudulent or suspicious charges; (b) cancelling and reissuing cards; (c) purchasing credit monitoring and identity theft prevention services; (d) attempting to withdraw funds linked to compromised, frozen accounts; (e) removing withdrawal and purchase limits on compromised accounts; (f) communicating with financial institutions to dispute fraudulent charges; (g) resetting automatic billing instructions and changing passwords; (h) freezing and unfreezing credit bureau account information; (i) cancelling and re-setting automatic payments as necessary; and (j) paying late fees and declined payment penalties as a result of failed automatic payments.

29. Additionally, Plaintiff and the Class have suffered or are at increased risk of suffering from, *inter alia*, the loss of the opportunity to control how their PII and PHI is used, the diminution in the value and/or use of their PII and PHI entrusted to Defendant, and loss of privacy.

[11] U.S. Dep't of Justice, *Victims of Identity Theft, 2014* (Nov. 13, 2017), http://www.bjs.gov/content/pub/pdf/vit14.pdf.

The Value of PII and PHI

30. It is well known that PII and PHI, and financial account information in particular, is an invaluable commodity and a frequent target of hackers.

31. According to Javelin Strategy & Research, in 2017 alone over 16.7 million individuals were affected by identity theft, causing $16.8 billion to be stolen.[12]

32. People place a high value not only on their PII and PHI, but also on the privacy of that data. This is because identity theft causes "significant negative financial impact on victims" as well as severe distress and other strong emotions and physical reactions.[13]

33. People are particularly concerned with protecting the privacy of their financial account information and social security numbers, which are the "secret sauce" that is "as good as your DNA to hackers."[14] There are long-term consequences to data breach victims whose social security numbers are taken and used by hackers. Even if they know their social security numbers have been accessed, Plaintiff and Class members cannot obtain new numbers unless they become a victim of social security

[12] Javelin Strategy & Research, *Identity Fraud Hits All Time High With 16.7 Million U.S. Victims in 2017, According to New Javelin Strategy & Research Study* (Feb. 6, 2018), https://www.javelinstrategy.com/press-release/identity-fraud-hits-all-time-high-167-million-us-victims-2017-according-new-javelin.

[13] Identity Theft Resource Center, *Identity Theft: The Aftermath 2017*, https://www.ftc.gov/system/files/documents/public_comments/2017/10/00004-141444.pdf.

[14] Cameron Huddleston, *How to Protect Your Kids From the Anthem Data Breach*, Kiplinger, (Feb. 10, 2015), https://www.kiplinger.com/article/credit/T048-C011-S001-how-to-protect-your-kids-from-the-anthem-data-brea.html.

number misuse. Even then, the Social Security Administration has warned that "a new number probably won't solve all [] problems … and won't guarantee … a fresh start."[15]

Industry Standards for Data Security

34. In light of the numerous high-profile data breaches targeting companies like Target, Neiman Marcus, eBay, Anthem, Deloitte, Equifax, and Capital One, Defendant is, or reasonably should have been, aware of the importance of safeguarding PII and PHI, as well as of the foreseeable consequences of its systems being breached.

35. Security standards commonly accepted among businesses that store PII and PHI using the internet include, without limitation:

a. Maintaining a secure firewall configuration;

b. Monitoring for suspicious or irregular traffic to servers;

c. Monitoring for suspicious credentials used to access servers;

d. Monitoring for suspicious or irregular activity by known users;

e. Monitoring for suspicious or unknown users;

f. Monitoring for suspicious or irregular server requests;

g. Monitoring for server requests for PII and PHI;

h. Monitoring for server requests from VPNs; and

i. Monitoring for server requests from Tor exit nodes.

[15] Social Security Admin., *Identity Theft and Your Social Security Number*, at 6-7, https://www.ssa.gov/pubs/EN-05-10064.pdf.

36. The U.S. Federal Trade Commission ("FTC") publishes guides for businesses for cybersecurity[16] and protection of PII and PHI[17] which includes basic security standards applicable to all types of businesses.

37. The FTC recommends that businesses:

a. Identify all connections to the computers where you store sensitive information.

b. Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks.

c. Do not store sensitive consumer data on any computer with an internet connection unless it is essential for conducting their business.

d. Scan computers on their network to identify and profile the operating system and open network services. If services are not needed, they should be disabled to prevent hacks or other potential security problems. For example, if email service or an internet connection is not necessary on a certain computer, a business should consider closing the ports to those services on that computer to prevent unauthorized access to that machine.

[16] Start with Security: A Guide for Business, FTC (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

[17] Protecting Personal Information: A Guide for Business, FTC (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting personalinformation.pdf.

e. Pay particular attention to the security of their web applications—the software used to give information to visitors to their websites and to retrieve information from them. Web applications may be particularly vulnerable to a variety of hack attacks.

f. Use a firewall to protect their computers from hacker attacks while it is connected to a network, especially the internet.

g. Determine whether a border firewall should be installed where the business's network connects to the internet. A border firewall separates the network from the internet and may prevent an attacker from gaining access to a computer on the network where sensitive information is stored. Set access controls—settings that determine which devices and traffic get through the firewall—to allow only trusted devices with a legitimate business need to access the network. Since the protection a firewall provides is only as effective as its access controls, they should be reviewed periodically.

h. Monitor incoming traffic for signs that someone is trying to hack in. Keep an eye out for activity from new users, multiple log-in attempts from unknown users or computers, and higher-than-average traffic at unusual times of the day.

i. Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly large amounts of data being transmitted from their system to an unknown user. If large amounts of information are being transmitted from a business' network, the transmission should be investigated to make sure it is authorized.

38. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer information, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.[18]

39. Because Defendant was entrusted with consumers' PII and PHI, it had, and has, a duty to consumers to keep their PII and PHI secure.

40. Consumers, such as Plaintiff and the Class, reasonably expect that when they provide PII and PHI to companies or when those companies forward their PII and PHI to companies such as Defendant, that their PII and PHI will be safeguarded.

[18] Federal Trade Commission, *Privacy and Security Enforcement: Press Releases*, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement.

41. Nonetheless, Defendant failed to prevent the Data Breach. Had Defendant properly maintained and adequately protected its systems, it could have prevented the Data Breach.

HIPAA Standards and Violations

42. Defendant is a covered entity under HIPAA as a business associate (45 C.F.R. § 160.103) and is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

43. In addition to failing to follow universal data security practices, Defendant failed to follow industry standard security practices, including:

a. Failing to protect against any reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. 164.306(a)(2);

b. Failing to ensure compliance with HIPAA security standards by its workforce or agents in violation of 45 C.F.R 164.306(a)(94);

c. Failing to effectively train all members of its workforce and its agents on the policies and procedures with respect to PHI as necessary to

maintain the security of PHI in violation of C.F.R. 164.530(b) and 45 C.F.R. 164.308(a)(5); and

d. Failing to design and implement and enforce policies and procedures to establish administrative safeguards to reasonably safeguard PHI in compliance with 45 C.F.R. 164.530(c).

IV. CLASS ACTION ALLEGATIONS

44. Plaintiff, individually and on behalf of all others, brings this class action pursuant to Fed. R. Civ. P. 23.

45. The proposed Class and Subclass are defined as follows:

> ***Nationwide Class****: All persons whose PII and PHI was maintained on Defendant's servers and was compromised in the Data Breach.*
>
> ***California Subclass:*** *All persons who are citizens of California whose PII and PHI was maintained on Defendant's servers and was compromised in the Data Breach.*

46. Plaintiff reserves the right to modify, change, or expand the definitions of the proposed Class based upon discovery and further investigation.

47. *Numerosity*: The proposed Class is so numerous that joinder of all members is impracticable. Although the precise number is not yet known to Plaintiff, Defendant has reported that the number of persons affected by the Data Breach is 1,509,616.[19] The Class members can be readily identified through Defendant's records.

[19] https://apps.web.maine.gov/online/aeviewer/ME/40/21846091-dc71-4ecc-9db8-a3be3e84a7d0.shtml

48. *Commonality*: Questions of law or fact common to the Class include, without limitation:

a. Whether Defendant owed a duty or duties to Plaintiff and the Class to exercise due care in collecting, storing, safeguarding, and obtaining their PII and PHI;

b. Whether Defendant breached that duty or those duties;

c. Whether Defendant failed to establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records to protect against known and anticipated threats to security;

d. Whether the security provided by Defendant was satisfactory to protect customer information as compared to industry standards;

e. Whether Defendant misrepresented or failed to provide adequate information to customers regarding the type of security practices used;

f. Whether Defendant knew or should have known that it did not employ reasonable measures to keep Plaintiff's and the Class's PII and PHI secure and prevent loss or misuse of that PII and PHI;

g. Whether Defendant acted negligently in connection with the monitoring and protecting of Plaintiff's and Class's PII and PHI;

h. Whether Defendant's conduct was intentional, willful, or negligent;

i. Whether Defendant violated any and all statutes and/or common law listed herein;

j. Whether the Class suffered damages as a result of Defendant's conduct, omissions, or misrepresentations; and

k. Whether the Class is entitled to injunctive, declarative, and monetary relief as a result of Defendant's conduct.

49. *Typicality*: The claims or defenses of Plaintiff are typical of the claims or defenses of the Class. Class members were injured and suffered damages in substantially the same manner as Plaintiff, Class members have the same claims against Defendant relating to the same course of conduct, and Class members are entitled to relief under the same legal theories asserted by Plaintiff.

50. *Adequacy*: Plaintiff will fairly and adequately protect the interests of the proposed Class and has no interests antagonistic to those of the proposed Class. Plaintiff has retained counsel experienced in the prosecution of complex class actions including, but not limited to, data breaches.

51. *Predominance*: Questions of law or fact common to proposed Class members predominate over any questions affecting only individual members. Common questions such as whether Defendant owed a duty to Plaintiff and the Class and whether Defendant breached its duties predominate over individual questions such as measurement of economic damages.

52. *Superiority*: A class action is superior to other available methods for the fair and efficient adjudication of these claims because individual joinder of the claims of the Class is impracticable. Many members of the Class are without the financial resources necessary to pursue this matter. Even if some members of the Class could afford to litigate their claims separately, such a result would be unduly burdensome to the courts in which the individualized cases would proceed. Individual litigation increases the time and expense of resolving a common dispute concerning Defendant's actions toward an entire group of individuals. Class action procedures allow for far fewer management difficulties in matters of this type and provide the unique benefits of unitary adjudication, economies of scale, and comprehensive supervision over the entire controversy by a single judge in a single court.

53. *Manageability*: Plaintiff is unaware of any difficulties that are likely to be encountered in the management of this action that would preclude its maintenance as a class action.

54. The Class may be certified pursuant to Rule 23(b)(2) because Defendant has acted on grounds generally applicable to the Class, thereby making appropriate final injunctive relief or corresponding declaratory relief with respect to the Class as a whole.

55. The Class may also be certified pursuant to Rule 23(b)(3) because questions of law and fact common to the Class will predominate over questions affecting individual members, and a class action is superior to other methods for fairly and

efficiently adjudicating the controversy and causes of action described in this Complaint.

56. Particular issues under Rule 23(c)(4) are appropriate for certification because such claims present particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein.

V. CAUSES OF ACTION

COUNT I
NEGLIGENCE
(on behalf of the Nationwide Class)

57. Plaintiff hereby incorporates by reference all preceding paragraphs as though fully set forth herein.

58. Defendant owed a duty of care to Plaintiff and Class members to use reasonable means to secure and safeguard the entrusted PII and PHI, to prevent its unauthorized access and disclosure, to guard it from theft, and to detect any attempted or actual breach of its systems. These common law duties existed because Plaintiff and Class members were the foreseeable and probable victims of any inadequate security practices. In fact, not only was it foreseeable that Plaintiff and Class members would be harmed by the failure to protect their PII and PHI because hackers routinely attempt to steal such information and use it for nefarious purposes, but Defendant knew that it was more likely than not Plaintiff and Class members would be harmed by such exposure of their PII and PHI.

59. Defendant's duties to use reasonable security measures also arose as a result of the special relationship that existed between Defendant, on the one hand, and Plaintiff and Class members, on the other hand. The special relationship arose because Plaintiff and Class members entrusted Defendant with their PII and PHI, Defendant accepted and held the PII and PHI, and Defendant represented that the PII and PHI would be kept secure pursuant to its data security policies. Defendant alone could have ensured that its data security systems and practices were sufficient to prevent or minimize the data breach.

60. Defendant's duties to use reasonable data security measures also arose under Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect PII and PHI. Various FTC publications and data security breach orders further form the basis of Defendant's duties. In addition, individual states have enacted statutes based upon the FTC Act that also created a duty.

61. Defendant's violations of Section 5 of the FTC Act constitute negligence per se.

62. Defendant breached the aforementioned duties when it failed to use security practices that would protect the PII and PHI provided to it by Plaintiff and Class

members, thus resulting in unauthorized third-party access to the Plaintiff's and Class members' PII and PHI.

63. Defendant further breached the aforementioned duties by failing to design, adopt, implement, control, manage, monitor, update, and audit its processes, controls, policies, procedures, and protocols to comply with the applicable laws and safeguard and protect Plaintiff's and Class members' PII and PHI within its possession, custody, and control.

64. As a direct and proximate cause of failing to use appropriate security practices, Plaintiff's and Class members' PII and PHI was disseminated and made available to unauthorized third parties.

65. Defendant admitted that Plaintiff's and Class members' PII and PHI was wrongfully disclosed as a result of the breach.

66. The breach caused direct and substantial damages to Plaintiff and Class members, as well as the possibility of future and imminent harm through the dissemination of their PII and PHI and the greatly enhanced risk of credit fraud or identity theft.

67. By engaging in the forgoing acts and omissions, Defendant committed the common law tort of negligence. For all the reasons stated above, Defendant's conduct was negligent and departed from reasonable standards of care including by, but not limited to: failing to adequately protect the PII and PHI; failing to conduct regular

security audits; and failing to provide adequate and appropriate supervision of persons having access to Plaintiff's and Class members' PII and PHI.

68. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and the Class, their PII and PHI would not have been compromised.

69. Neither Plaintiff nor the Class contributed to the breach or subsequent misuse of their PII and PHI as described in this Complaint. As a direct and proximate result of Defendant's actions and inactions, Plaintiff and the Class have been put at an increased risk of credit fraud or identity theft, and Defendant has an obligation to mitigate damages by providing adequate credit and identity monitoring services. Defendant is liable to Plaintiff and the Class for the reasonable costs of future credit and identity monitoring services for a reasonable period of time, substantially in excess of one year. Defendant is also liable to Plaintiff and the Class to the extent that they have directly sustained damages as a result of identity theft or other unauthorized use of their PII and PHI, including the amount of time Plaintiff and the Class have spent and will continue to spend as a result of Defendant's negligence. Defendant is also liable to Plaintiff and the Class to the extent their PII and PHI has been diminished in value because Plaintiff and the Class no longer control their PII and PHI and to whom it is disseminated.

COUNT II
INVASION OF PRIVACY
(on behalf of the Nationwide Class)

70. Plaintiff hereby incorporates by reference all preceding paragraphs as though fully set forth herein.

71. Plaintiff and Class members have objective reasonable expectations of solitude and seclusion in their personal and private information and the confidentiality of the content of personal information and non-public medical information.

72. Defendant invaded Plaintiff's and the Class's right to privacy by allowing the unauthorized access to their PII and PHI and by negligently maintaining the confidentiality of Plaintiff's and the Class's PII and PHI, as set forth above.

73. The intrusion was offensive and objectionable to Plaintiff, the Class, and to a reasonable person of ordinary sensibilities in that Plaintiff's and the Class's PII and PHI was disclosed without prior written authorization from Plaintiff and the Class.

74. The intrusion was into a place or thing which was private and is entitled to be private, in that Plaintiff and the Class provided and disclosed their PII and PHI to Defendant privately with an intention that the PII and PHI would be kept confidential and protected from unauthorized disclosure. Plaintiff and the Class were reasonable to believe that such information would be kept private and would not be disclosed without their written authorization.

75. As a direct and proximate result of Defendant's above acts, Plaintiff's and the Class's PII and PHI was viewed, distributed, and used by persons without prior written authorization and Plaintiff and the Class suffered damages as described herein.

76. Defendant is guilty of oppression, fraud, or malice by permitting the unauthorized disclosure of Plaintiff's and the Class's PII and PHI with a willful and conscious disregard of their right to privacy.

77. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause Plaintiff and the Class great and irreparable injury in that the PII and PHI maintained by Defendant can be viewed, printed, distributed, and used by unauthorized persons. Plaintiff and the Class have no adequate remedy at law for the injuries in that a judgment for the monetary damages will not end the invasion of privacy for Plaintiff and the Class, and Defendant may freely treat Plaintiff's and the Class's PII and PHI with sub-standard and insufficient protections.

COUNT III
BREACH OF FIDUCIARY DUTY
(on behalf of the Nationwide Class)

78. Plaintiff hereby incorporates by reference all preceding paragraphs as though fully set forth herein.

79. As alleged above, Plaintiff and the Class had agreements with Defendant, both express and implied, that required Defendant to keep their PII and PHI confidential.

80. The parties had a fiduciary relationship of trust and confidence such that Plaintiff and the Class relied and depended on Defendant to securely maintain their highly sensitive PII and PHI, and Defendant had a duty of care to safeguard Plaintiff's and the Class's PII and PHI.

81. Defendant breached that confidence by disclosing Plaintiff's and the Class's PII and PHI without their authorization and for unnecessary purposes.

82. As a result of the data breach, Plaintiff and the Class suffered damages that were attributable to Defendant's failure to maintain confidence in their PII and PHI.

COUNT IV
UNJUST ENRICHMENT
(on behalf of the Nationwide Class)

83. Plaintiff hereby incorporates by reference all preceding paragraphs as though fully set forth herein.

84. Plaintiff and the Class have an interest, both equitable and legal, in their PII and PHI that was conferred upon, collected by, and maintained by Defendant and that was ultimately compromised in the data breach.

85. Defendant, by way of its acts and omissions, knowingly and deliberately enriched itself by saving the costs it reasonably should have expended on security measures to secure Plaintiff's and the Class's PII and PHI.

86. Defendant also understood and appreciated that the PII and PHI pertaining to Plaintiff and the Class was private and confidential and its value depended upon Defendant maintaining the privacy and confidentiality of that PII and PHI.

87. Instead of providing for a reasonable level of security that would have prevented the breach—as is common practice among companies entrusted with such PII and PHI—Defendant instead consciously and opportunistically calculated to increase its own profits at the expense of Plaintiff and the Class. Nevertheless, Defendant continued to obtain the benefits conferred on it by Plaintiff and the Class. The benefits conferred upon, received, and enjoyed by Defendant were not conferred officiously or gratuitously, and it would be inequitable and unjust for Defendant to retain these benefits.

88. Plaintiff and the Class, on the other hand, suffered as a direct and proximate result. As a result of Defendant's decision to profit rather than provide requisite security, and the resulting breach disclosing Plaintiff's and the Class's PII and PHI, Plaintiff and the Class suffered and continue to suffer considerable injuries in the forms of, *inter alia,* attempted identity theft, time and expenses mitigating harms, diminished value of PII and PHI, loss of privacy, and increased risk of harm.

89. Thus, Defendant engaged in opportunistic conduct in spite of its duties to Plaintiff and the Class, wherein it profited from interference with Plaintiff's and the Class's legally protected interests. As such, it would be inequitable, unconscionable,

and unlawful to permit Defendant to retain the benefits it derived as a consequence of its conduct.

90. Accordingly, Plaintiff, on behalf of himself and the Class, respectfully request that this Court award relief in the form of restitution or disgorgement in the amount of the benefit conferred on Defendant as a result of its wrongful conduct, including specifically, the amounts that Defendant should have spent to provide reasonable and adequate data security to protect Plaintiff's and the Class's PII and PHI, and/or compensatory damages.

COUNT V
VIOLATION OF THE CALIFORNIA CONFIDENTIALITY OF MEDICAL INFORMATION ACT ("CMIA")
Cal. Civ. Code § 56, et seq
(on behalf of the California Subclass)

91. Plaintiff, on behalf of himself and the California Subclass, restates and realleges all proceeding allegations above and hereafter as if fully set forth herein.

92. Defendant is "a provider of health care," as defined in Cal. Civ. Code §56.05(m) and/or a "contractor" as defined in California Civil Code section 56.05(d), and is therefore subject to the requirements of the CMIA, Cal. Civ. Code §56.10(a), (d) and (e), 56.36(b), 56.101(a) and (b).

93. As a provider of health care or a contractor, Defendant is required by the CMIA to ensure that medical information regarding patients is not disclosed or disseminated and/or released without patient's authorization, and to protect and preserve

the confidentiality of the medical information regarding a patient, under Civil Code §§ 56.06, 56.10, 56.13, 56.20, 56.245, 56.26, 56.35, 56.36, and 56.101.

94. As a provider of health care or a contractor, Defendant is required by the CMIA not to disclose medical information regarding a patient without first obtaining an authorization under Civil Code §§ 56.06, 56.10, 56.13, 56.20, 56.245, 56.26, 56.35, and 56.104.

95. Defendant is a person/entity licensed under California's Business and Professions Code, Division 2. See Cal. Bus. Prof. Code § 4000, et seq.

96. Plaintiff and Class Members are "patients" as defined in CMIA, Cal. Civ. Code §56.05(k) ("'Patient' means any natural person, whether or not still living, who received health care services from a provider of health care and to whom medical information pertains").

97. Furthermore, Plaintiff and Class Members, as patients and customers of Defendant, had their individually identifiable "medical information," within the meaning of Civil Code § 56.05(j), created, maintained, preserved, and stored on Defendant's computer network, and were patients on or before the date of the Data Breach.

98. Defendant disclosed "medical information," as defined in CMIA, Cal. Civ. Code § 56.05(j), to unauthorized persons without first obtaining consent, in violation of Cal. Civ. Code § 56.10(a). The disclosure of information to unauthorized individuals in

the Data Breach resulted from the affirmative actions of Defendant's employees, which allowed the hackers to see and obtain Plaintiff's and Class Members' medical information.

99. Defendant negligently created, maintained, preserved, stored, and then exposed Plaintiff's and Class Members' individually identifiable "medical information," within the meaning of Cal. Civ. Code § 56.05(j), including Plaintiff's and Class members' names, addresses, medical information, and health insurance information, that alone or in combination with other publicly available information, reveals their identities. Specifically, Defendant knowingly allowed and affirmatively acted in a manner that allowed unauthorized parties to access, exfiltrate, and actually view Plaintiff's and Class Members' confidential Private Information.

100. Defendant's negligence resulted in the release of individually identifiable medical information pertaining to Plaintiff and Class Members to unauthorized persons and the breach of the confidentiality of that information. Defendant's negligent failure to maintain, preserve, store, abandon, destroy, and/or dispose of Plaintiff's and Class Members' medical information in a manner that preserved the confidentiality of the information contained therein, in violation of Cal. Civ. Code §§ 56.06 and 56.101(a).

101. Defendant also violated Sections 56.06 and 56.101 of the CMIA, which prohibit the negligent creation, maintenance, preservation, storage, abandonment, destruction, or disposal of confidential personal medical information.

102. Plaintiff's and Class Members' medical information was accessed and actually viewed by hackers in the Data Breach.

103. Plaintiff's and Class Members' medical information that was the subject of the Data Breach included "electronic medical records" or "electronic health records" as referenced by Civil Code § 56.101(c) and defined by 42 U.S.C. § 17921(5).

104. Defendant's computer systems did not protect and preserve the integrity of electronic medical information in violation of Cal. Civ. Code § 56.101(b)(1)(A). As a direct and proximate result of Defendant's above-noted wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, and violation of the CMIA, Plaintiff and the Class Members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, inter alia:

a. present, imminent, immediate and continuing increased risk of identity theft, identity fraud and medical fraud –risks justifying expenditures for protective and remedial services for which they are entitled to compensation;

b. invasion of privacy;

c. breach of the confidentiality of the PHI;

d. statutory damages under the California CMIA;

e. deprivation of the value of their PHI, for which there is well-established national and international markets; and/or,

f. the financial and temporal cost of monitoring their credit, monitoring their financial accounts, and mitigating their damages.

105. As a direct and proximate result of Defendant's wrongful actions, inaction, omission, and want of ordinary care that directly and proximately caused the release of Plaintiff's and Class Members' Private Information, Plaintiff's and Class Members' personal medical information was viewed by, released to, and disclosed to third parties without Plaintiff's and Class Members' written authorization.

106. Defendant's negligent failure to maintain, preserve, store, abandon, destroy, and/or dispose of Plaintiff's and Class Members' medical information in a manner that preserved the confidentiality of the information contained therein violated the CMIA.

107. Plaintiff and the Class Members were injured and have suffered damages, as described above, from Defendant's illegal and unauthorized disclosure and negligent release of their medical information in violation of Cal. Civ. Code §§56.10 and 56.101, and therefore seek relief under Civ. Code §§ 56.35 and 56.36, which allows for actual damages, nominal statutory damages of $1,000, punitive damages of $3,000, injunctive relief, and attorneys' fees, expenses, and costs.

COUNT VI
INVASION OF PRIVACY
Cal. Const. Art. 1 § 1
(on behalf of the California Subclass)

108. Plaintiff, on behalf of himself and the California Subclass, restates and realleges all proceeding allegations above and hereafter as if fully set forth herein.

109. California established the right to privacy in Article I, Section 1 of the California Constitution.

110. Plaintiff and the Subclass had a legitimate expectation of privacy to their PII and PHI and were entitled to the protection of this information against disclosure to unauthorized third parties.

111. Defendant, headquartered in California and offering its services from California, owed a duty to Plaintiff and the Subclass to keep their Private Information confidential.

112. Defendant failed to protect and released to unknown and unauthorized third parties the PII and PHI of Plaintiff and the Subclass Members.

113. Defendant enabled and allowed unauthorized and unknown third parties access to and examination of the Private Information of Plaintiff and the Subclass Members, by way of Defendant's failure to protect the PII and PHI.

114. The unauthorized release to, custody of, and examination by unauthorized third parties of the Private Information of Plaintiff and the Subclass Members is highly offensive to a reasonable person.

115. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiff and the Subclass Members disclosed their Private Information to Defendant as part of their medical care or employment with Defendant, but privately with an intention that the Private Information would be kept confidential and would be protected from unauthorized disclosure.

116. Plaintiff and the Subclass Members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

117. The Data Breach at the hands of Defendant constitutes an intentional interference with Plaintiff's and the Subclass's interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

118. Defendant acted with a knowing state of mind when it permitted the Data Breach to occur because it was with actual knowledge that its information security practices were inadequate and insufficient.

119. Because Defendant acted with this knowing state of mind, it had notice and knew the inadequate and insufficient information security practices would cause injury and harm to Plaintiff and the Subclass Members.

120. As a proximate result of the above acts and omissions of Defendant, the Private Information of Plaintiff and the Subclass Members was disclosed to third

parties without authorization, causing Plaintiff and the Subclass to suffer damages.

121. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Subclass Members in that the PII and PHI maintained by Defendant can be viewed, distributed, and used by unauthorized persons for years to come. Plaintiff and the Subclass Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiff and the Subclass.

COUNT VII
CALIFORNIA CONSUMER RECORDS ACT
Cal. Civ. Code § 1798.82, et seq.
(on behalf of California Subclass)

122. Plaintiff, on behalf of himself and the California Subclass, restates and realleges all allegations of the preceding paragraphs as though fully set forth herein.

123. Section 1798.2 of the California Civil Code requires any "person or business that conducts business in California, and that owns or licenses computerized data that includes personal information" to "disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Under section 1798.82, the disclosure "shall be made in the most expedient time possible and without unreasonable delay. "

124. The CCRA further provides: "Any person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person." (Cal. Civ. Code, § 1798.82(b)).

125. Any person or business that is required to issue a security breach notification under the CCRA shall meet all of the following requirements:

a. The security breach notification shall be written in plain language;

b. The security breach notification shall include, at a minimum, the following information:

- The name and contact information of the reporting person or business subject to this section;
- A list of the types of personal information that were or are reasonably believed to have been the subject of a breach;

c. If the information is possible to determine at the time the notice is provided, then any of the following:

- The date of the breach;
- The estimated date of the breach; or
- The date range within which the breach occurred. The notification

shall also include the date of the notice.

d. Whether notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided;

e. A general description of the breach incident, if that information is possible to determine at the time the notice is provided; and

f. The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a Social Security number or a driver's license or California identification card number.

126. The Data Breach described herein constituted a "breach of the security system" of Defendant.

127. As alleged above, Defendant unreasonably delayed informing Plaintiff and Subclass Members about the Data Breach, affecting their PII and PHI, after Defendant knew the Data Breach had occurred.

128. Defendant failed to disclose to Plaintiff and the Subclass Members, without unreasonable delay and in the most expedient time possible, the breach of security of their unencrypted, or not properly and securely encrypted, PII and PHI when Defendant knew or reasonably believed such information had been compromised.

129. Defendant's ongoing business interests gave Defendant incentive to conceal the Data Breach from the public to ensure continued revenue.

130. Upon information and belief, no law enforcement agency instructed Defendant that timely notification to Plaintiff and the Subclass Members would impede its investigation.

131. As a result of Defendant's violation of California Civil Code section 1798.82, Plaintiff and the Subclass Members were deprived of prompt notice of the Data Breach and were thus prevented from taking appropriate protective measures, such as securing identity theft protection or requesting a credit freeze. These measures could have prevented some of the damages suffered by Plaintiff and Subclass members because their stolen information would have had less value to identity thieves.

132. As a result of Defendant's violation of California Civil Code section 1798.82, Plaintiff and the Subclass Members suffered incrementally increased damages separate and distinct from those simply caused by the Data Breach itself.

133. Plaintiff and the Subclass Members seek all remedies available under California Civil Code section 1798.84, including, but not limited to the damages suffered by Plaintiff and the other Subclass Members, including but not limited to benefit-of-the-bargain and time spent monitoring their accounts for identity theft and medical identity theft, and equitable relief.

134. Defendant's misconduct as alleged herein is fraud under California Civil Code section 3294(c)(3) in that it was deceit or concealment of a material fact known to the Defendant conducted with the intent on the part of Defendant of depriving

Plaintiff and the Subclass Members of "legal rights or otherwise causing injury." In addition, Defendant's misconduct as alleged herein is malice or oppression under California Civil Code section 3294(c)(1) and (c) in that it was despicable conduct carried on by Defendant with a willful and conscious disregard of the rights or safety of Plaintiff and the Subclass Members and despicable conduct that has subjected Plaintiff and the Subclass Members to cruel and unjust hardship in conscious disregard of their rights. As a result, Plaintiff and the Subclass Members are entitled to punitive damages against Defendant under California Civil Code section 3294(a).

COUNT VIII
CALIFORNIA UNFAIR COMPETITION LAW
Cal. Bus. & Prof. Code § 17200, et seq.
(on behalf of the California Subclass)

135. Plaintiff, on behalf of himself and the California Subclass, restates and realleges all allegations of the preceding paragraphs as though fully set forth herein.

136. Defendant regularly does business in California. Defendant violated California's Unfair Competition Law ("UCL") (Cal. Bus. & Prof. Code, § 17200, et seq.) by engaging in unlawful, unfair, or fraudulent business acts and practices and unfair, deceptive, untrue or misleading advertising that constitute acts of "unfair competition" as defined in the UCL, including, but not limited to, the following:

a. by representing and advertising that it would maintain adequate data privacy and security practices and procedures to safeguard PII and PHI from unauthorized disclosure, release, data breach, and theft; representing

and advertising that it did and would comply with the requirement of relevant federal and state laws pertaining to the privacy and security of the Subclass's PII and PHI; and omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for the Subclass's PII and PHI;

b. by soliciting and collecting Subclass members' PII and PHI with knowledge that the information would not be adequately protected; and by storing Plaintiff's and Subclass Members' PII and PHI in an unsecure electronic environment;

c. by failing to disclose the Data Breach in a timely and accurate manner, in violation of California Civil Code section 1798.82;

d. by violating the privacy and security requirements of HIPAA, 42 U.S.C. §1302d, et seq.;

e. by violating the CMIA, California Civil Code section 56, et seq.; and

f. by violating the CCRA, California Civil Code section 1798.82.

137. These unfair acts and practices were immortal, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiffs and Subclass Members. Defendant's practice was also contrary to legislatively declared and public policies that seek to protect consumer data and ensure that entities who solicit or are entrusted with personal data utilize appropriate security measures, as reflected by laws

like the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1302d, et seq., CMIA, Cal. Civ. Code, § 56, et seq., and the CCRA, Cal. Civ. Code, § 1798.81.5.

138. As a direct and proximate result of Defendant's unfair and unlawful practices and acts, Plaintiff and the Subclass Members were injured and lost money or property, including but not limited to the overpayments Defendant received to take reasonable and adequate security measures (but did not), the loss of their legally protected interest in the confidentiality and privacy of their PII and PHI, and additional losses described above.

139. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard Plaintiff's and Subclass Members' PII and PHI and that the risk of a data breach or theft was highly likely. Defendant's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of the Class.

140. Plaintiff seeks relief under the UCL, including restitution to the Subclass of money or property that the Defendant may have acquired by means of Defendant's deceptive, unlawful, and unfair business practices, declaratory relief, attorney fees, costs and expenses (pursuant to Cal. Code Civ. Proc., § 1021.5), and injunctive or other equitable relief.

COUNT VIII
CALIFORNIA CONSUMER PRIVACY ACT ("CCPA")
Cal. Civ. Code § 1798, *et seq.*
(On behalf of the California Subclass)

141. Plaintiff, on behalf of himself and the California Subclass, restates and realleges all allegations of the preceding paragraphs as though fully set forth herein.

142. The California Legislature has explained: "The unauthorized disclosure of personal information and the loss of privacy can have devasting effects for individuals, ranging from financial fraud, identity theft, and unnecessary costs to personal time and finances, to destruction of property, harassment, reputational damage, emotional stress, and even potential physical harm."[20]

143. The CCPA imposes an affirmative duty on businesses that maintain personal information about California residents to implement and maintain reasonable security procedures and practices that are appropriate to the nature of the information collected. Defendant failed to implement such procedures which resulted in the Data Breach.

144. It also requires "[a] business that discloses personal information about a California resident pursuant to a contract with a nonaffiliated third party . . . [to] require by contract that the third party implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal

[20] California Consumer Privacy Act (CCPA) Compliance, https://buyergenomics.com/ccpa-complience/.

information from unauthorized access, destruction, use, modification, or disclosure." Cal. Civ. Code § 1798.81.5(c).

145. Section 1798.150(a)(1) of the CCPA provides: "Any consumer whose nonencrypted or nonredacted personal information, as defined [by the CCPA] is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for" statutory or actual damages, injunctive or declaratory relief, and any other relief the court deems proper.

146. Plaintiff and California Subclass members are "consumer[s]" as defined by Civ. Code § 1798.140(g) because they are "natural person[s] who [are] California resident[s], as defined in Section 17014 of Title 18 of the California Code of Regulations, as that section read on September 1, 2017."

147. Defendant is a "business" as defined by Civ. Code § 1798.140(c) because Defendant:

a. is a "sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners";

b. "collects consumers' personal information, or on the behalf of which is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information";

c. does business in California; and

d. has annual gross revenues in excess of $25 million; annually buys, receives for the business' commercial purposes, sells or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices; or derives 50 percent or more of its annual revenues from selling consumers' personal information.

148. The Private Information taken in the Data Breach is personal information as defined by Civil Code § 1798.81.5(d)(1)(A) because it contains Plaintiff's and California Subclass members' unencrypted first and last names and Social Security numbers among other information.

149. Plaintiff and California Subclass members' Private Information was subject to unauthorized access and exfiltration, theft, or disclosure because their PII, including name and contact information was wrongfully taken, accessed, and viewed by unauthorized third parties.

150. The Data Breach occurred as a result of Defendant's failure to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect Plaintiff's and California Subclass members' PII. Defendant

failed to implement reasonable security procedures to prevent an attack on their server or network, including its email system, by hackers and to prevent unauthorized access of Plaintiff's and California Subclass members' PII as a result of this attack.

151. Simultaneously herewith, Plaintiff is providing notice to Defendant pursuant to Cal. Civ. Code § 1798.150(b)(1), identifying the specific provisions of the CCPA Plaintiff alleges Keenan has violated or is violating. Although a cure is not possible under the circumstances, if (as expected) Keenan is unable to cure or does not cure the violation within 30 days, Plaintiff will amend this Complaint to pursue actual or statutory damages as permitted by Cal. Civ. Code § 1798.150(a)(1)(A).

152. Plaintiff seeks all relief available under the CCPA including damages to be measured as the greater of actual damages or statutory damages in an amount up to seven hundred and fifty dollars ($750) per consumer per incident. See Cal. Civ. Code § 1798.150(a)(1)(A) & (b).

153. As a result of Defendant's failure to implement and maintain reasonable security procedures and practices that resulted in the Data Breach, Plaintiff seeks injunctive relief, including public injunctive relief, declaratory relief, and any other relief as deemed appropriate by the Court.

VI. PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all others similarly situated, prays for a judgment against Defendant as follows:

a. For an order certifying the proposed Class, appointing Plaintiff as Representative of the proposed Class, and appointing the law firms representing Plaintiff as counsel for the Class;

b. For compensatory and punitive and treble damages in an amount to be determined at trial;

c. Payment of costs and expenses of suit herein incurred;

d. Both pre-and post-judgment interest on any amounts awarded;

e. Payment of reasonable attorneys' fees and expert fees;

f. Such other and further relief as the Court may deem proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands trial by jury,

Dated: March 1, 2024

Respectfully submitted,

/s/ John J. Nelson

John J. Nelson (SBN 317598)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
280 S. Beverly Drive
Beverly Hills, CA 90212
Telephone: (858) 209-6941
Email: jnelson@milberg.com

Jeffrey S. Goldenberg
GOLDENBERG SCHNEIDER, LPA
4445 Lake Forest Drive, Suite 490
Cincinnati, OH 45242

Telephone: (513) 345-8291
jgoldenberg@gs-legal.com

Charles E. Schaffer
LEVIN SEDRAN & BERMAN, LLP
510 Walnut Street, Suite 500
Philadelphia, PA 19106
Tel: 215-592-1500
Fax: 215-592-4663
cschaffer@lfsblaw.com

Counsel for Plaintiff and Proposed Class